Jak być bezpiecznym w internecie?

Zuzanna Nowak 8B

1.Chroń swoje dane osobowe

- Ludzie pokazują zbyt wiele w internecie, chwaląc się np. zdanym prawem jazdy lub nowym dowodem. Czy wiesz, że takie działania mogą mieć bardzo poważne konsekwencje? W ten sposób złodzieje bardzo szybko identyfikują swoją ofiarę, ponieważ mogą poznać numer PESEL, adres zamieszkania i inne dane, które następnie wykorzystują do działań przestępczych.

https://tp.com.pl/static/files/gallery/157/1283487_1646641619.jpg

2.Aktualizuj swój program antywirusowy

W każdej chwili możesz stać się ofiarą cyberataku. Zabezpiecz swoje urządzenia elektroniczne (komputer, tablet, smartfon) programem antywirusowym i regularnie go aktualizuj. Bądź o krok przed oszustami i nie daj się zaskoczyć.

https://brief.pl/wp-content/uploads/2021/02/Jak-byc-bezpiecznym-w-internecie_.jpg

3. Zawsze ustawiaj silne hasła

Pamiętaj, że jest to pierwsza bariera z jaką musi się spotkać cyberoszust, w trakcie próby włamania się na Twoje konto. Spraw by była twierdzą nie do zdobycia. Tam gdzie to możliwe włącz opcję logowania dwuetapowego.

https://www.purepc.pl/files/Image/ArtykulHeadlines/11363.jpg

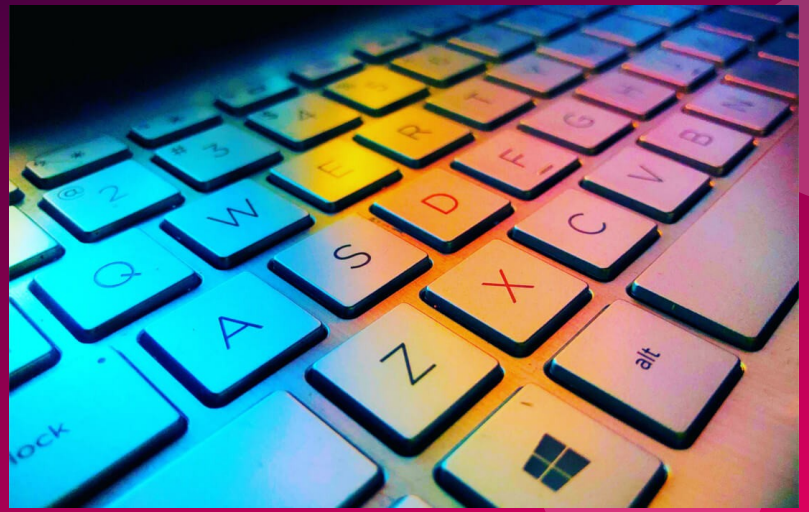
4.Uważaj na fake newsy

Cokolwiek czytasz, daj sobie czas na sprawdzenie źródła, autorów. Cyberprzestępcy będą grać na twoich emocjach oraz będą tobą manipulować produkując „fake newsy” którym łatwo uwierzyć.

https://www.sp12dg.pl/strona/wp-content/uploads/2022/03/komp.jpg

5.Uważaj na wiadomości i linki nieznanego pochodzenia

Nigdy nie otwieraj wiadomości i załączonych do nich linków z nieznanych źródeł.



https://justjoin.it/blog/storage/2020/08/klawiatura-haslo-1100x700-1.jpg

6.Zawsze twórz kopie zapasową

Tworzenie kopii zapasowych danych to nic innego jak dodatkowe zabezpieczenie twoich plików. Służy ono do odtworzenia oryginalnych danych w przypadku ich utraty.

https://www.jezyk.com.pl/wp-content/uploads/2024/03/006e-jezyk-baza-wiedzy-co-to-jest-bezpieczenstwo-w-sieci.jpg

7.Unikaj publicznych sieci Wi-Fi

Korzystanie z publicznych sieci Wi-Fi jest wygodne,ale może narażać użytkowników na znaczne ryzyko, gdyż najczęściej nie są one odpowiednio zabezpieczone,stając się łatwym celem dla ataków typu „man-in-the-middle”gdzie hakerzy mogą przechwytywać przesyłane dane.

https://phavi.umcs.pl/ph/r,1024,800/agicon/c/2023/0831/570324364f040efea368.jpg

8.Nie otwieraj dziwnie wyglądających wiadomości

Wśród czających się na nas w sieci zagrożeń, warto zwrócić uwagę na te,które samodzielnie na siebie sprowadzamy. Maile z prośbą o kliknięcie i natychmiastowe zalogowanie się do banku,podejrzanie atrakcyjne ceny w sklepie z nadesłanego linku, zachęta do obejrzenia zdjęć lub filmów.

https://rynekinformacji.pl/wp-content/uploads/2021/10/data-protection-4394633_1920.jpg

9.Zgłaszaj próby oszustwa

Jeżeli coś budzi Twoje wątpliwości, poinformuj
o tym CERT Polska! Takie zgłoszenie pomoże chronić innych!

https://www.komputerwfirmie.org/wp-content/uploads/2021/06/wyciek_danych_w_sieci-1024x641-1.jpg

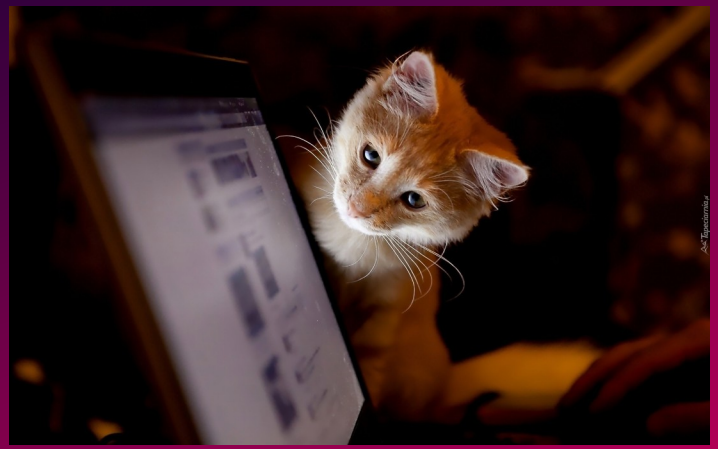
10.Zachowaj ostrożność

Z ostrożnością podchodź do linków i załączników, które otrzymasz w wiadomości, jeśli nie wiesz, od kogo pochodzą i co się w nich znajduje.

https://www.xdr.pl/media/k2/items/cache/f4b6dca0e2911082f0eb6e1df1a0e11d_XL.jpg

Dziękuje za uwagę!

Zuzanna Nowak 8B



https://www.tapeciarnia.pl/tapety/normalne/106466_kotek_monitor_informatyk_rudy.jpg